Enfoque UTE, V.4-N.2, Dic.2013: pp. 77 - 94
Recibido (Received): 2013/10/02
Aceptado (Accepted): 2013/12/13

http://ingenieria.ute.edu.ec/enfoqueute/
ISSN: 1390-6542

Gestión del riesgo en las metodologías de proyectos de tecnologías de información y comunicaciones

*(*Risk management in methodologies of information technology and communications projects*)*

Jonathan Carrillo Sánchez[1]

Resumen:
En la actualidad existen metodologías que presentan varios métodos para gestionar proyectos de Tecnologías de Información y Comunicaciones. Sin embargo, éstas no abarcan una solución integral para las opciones y eventos tecnológicos que se pueden presentar en la industria, Gobierno, Educación, entre otras. En el mercado existen varios modelos que identifican y analizan los riesgos según aspectos relevantes de su área de especialidad como por ejemplo: en proyectos, en desarrollo de software, comunicaciones, seguridad de la información y alineamiento con el negocio. Por tal motivo, esta investigación realizó una evaluación de las actividades de gestión del riesgo de las principales metodologías para conocer cuál de ellas abarca mayor correspondencia utilizando como parámetros elementos básicos de TI y una escala de valoración.

Palabras clave: TI; gobierno electrónico; marco de trabajo; comercio electrónico; gobierno de TI

Abstract:
At present there are methodologies that have several alternatives and methods to manage projects of Information and Communication Technologies. However, these do not cover a solution for the technology events that can occur in the industry, government, education, among others. In the technology market there are several models to identify and analyze risks according to relevant aspects of their area of specialty e.g. projects, in software development, communications, information security and business alignment. For this reason, this research conducted an evaluation of risk management activities of the methodologies used mostly to know which of them includes more correspondence with basic elements of IT using a rating scale.

Keywords:
IT; e-government; framework; e-commerce; IT government

1. Introducción

Luego del proceso de licitación, planificación e inicio de los proyectos, existen eventos o condiciones inciertas que producen efectos que pueden ser favorables o perjudiciales sobre al menos un objetivo del proyecto como: tiempo, coste, alcance, calidad y uso eficiente de los recursos. Esto se debe ya que muchos de los administradores de contrato o líderes de proyecto

[1] Universidad Tecnológica Equinoccial, Facultad de Ciencias de la Ingeniería, Quito – Ecuador (csjp101556@ ute.edu.ec)

no consideran planes de gerencia, análisis de riesgos, monitoreo, o porque no existe una política de gestión institucional que asegure el cumplimiento de estándares.

Por lo tanto, el objetivo de este documento es evaluar un conjunto de metodologías[2] de Tecnologías de Información y Comunicaciones, y presentar los resultados para conocer cuál de ellas alcanza mayor valoración respecto a la gestión del riesgo. Las metodologías que conciernen a esta investigación son: CMMI, SPICE, PMBOK, PRINCE2, COBIT 4.1[3], RISK IT, OCTAVE, NIST 800-30 y MAGERIT.

2. Metodologías presentadas

La Gestión del Riesgo es una de las áreas de gestión que las metodologías presentan para que los líderes o administradores de proyectos entreguen productos de calidad, en el tiempo previsto y dentro del presupuesto.

Con el fin de tener una visión global del riesgo tecnológico y de la gestión que se debe aplicar a los proyectos, es fundamental presentar y analizar conceptos básicos:

RIESGO

Boehm (1991) define exposición al riesgo como "**un valor compuesto, resultante de la multiplicación de la probabilidad de ocurrencia de un evento por la pérdida que la misma implica**".

Tomando como referencia la definición anterior, existen tres entidades básicas en el riesgo.

La Primera es que **el riesgo implica probabilidad**. Esta probabilidad se encuentra reflejada en eventos que pueden materializarse y se encuentran registradas como datos históricos, indicadores de mercado e información de expertos.

La segunda es que **el riesgo implica frecuencia**, es decir, el número de veces que una condición ha ocurrido. Esta también puede ser definida de manera cualitativa mediante condiciones como Frecuente, Normal o Poco Frecuente.

La tercera es que **el riesgo es universal** y el resultado son consecuencias que impactan a algún componente de un proyecto o de una actividad, siendo estos la programación, costos, calidad y alcance de los objetivos.

Por lo tanto, el riesgo es definido mediante la siguiente ecuación:

---

[2] Metodología es un término que en este documento puede ser denominado también como "Mejor Práctica"
[3] En esta investigación se analiza la versión 4.1 de COBIT, sin embargo, ISACA ha evolucionado el concepto de gobernanza de TI con la elaboración de la versión 5, que integra los siguientes Framewoks: COBIT, Val IT, RISK IT, ITAF y BMIS .

Riesgo = Probabilidad * Impacto (1)

Es importante indicar que la ecuación anterior puede aplicarse en un entorno cuantitativo y/o cualitativo.

GESTIÓN DEL RIESGO

Según Connell (1997): La Gestión del Riesgo de un Proyecto **"es identificar, estudiar y eliminar las fuentes de riesgo antes de que empiecen a amenazar la finalización satisfactoria de un proyecto"**. Por su parte Galaway (2004) define la Gestión de riesgos de un proyecto como "**el arte y la ciencia de identificar, analizar, y responder a los riesgos a lo largo de la vida de un proyecto, con el propósito de lograr los objetivos del proyecto"**.

De los dos conceptos anteriores, para lograr éxito en los proyectos mediante la Gestión del Riesgo, existen tres procesos básicos: identificación, análisis (estudio) y respuesta (manejo) del riesgo.

A base de los conceptos anteriores podemos deducir que en la **Identificación del Riesgo** se debe tomar en cuenta las fuentes que pueden incidir en la aparición de los riesgos los cuales pueden afectar a las actividades de los proyectos. Estos factores pueden ser económicos, sociales, de orden público, políticos, legales, cambios tecnológicos, estructura organizacional, sistemas de información, procesos, recursos económicos, entre otros.

Para la identificación puede utilizarse diferentes fuentes de información que pueden ser de la organización o de estudios que se han realizado tales como: registros históricos, opiniones de especialistas y expertos, informes de años anteriores, entrevistas, reuniones de trabajo, uso de diagramas de flujo, análisis y revisiones periódicas de factores económicos y tecnológicos, estadísticas, rankings, entre otros.

En el **Análisis del Riesgo** el objetivo es establecer una valoración y priorización de los riesgos a base de información obtenida en el proceso de identificación y de esta manera establecer el nivel de riesgo y las acciones que se van a implementar en el siguiente proceso. Para esto la probabilidad de ocurrencia y el impacto son valores necesarios que deben establecerse en escala de valoraciones sean estas cuantitativas o cualitativas.

La **Respuesta o Manejo del Riesgo** se refiere a la toma de decisiones entorno a las salvedades y salvaguardas para minimizar pérdidas. Existen riesgos que pueden ser aceptados y aquellos que no lo son, se los mitigará, transferirá o evitará mediante un análisis costo–beneficio y dentro de los parámetros técnico–legales.

La guía de PMBOK relaciona el concepto de Gestión del Riesgo con los procesos del ciclo de vida de un proyecto. PMBOK establece que existe mayor probabilidad de riesgo en la planificación del

proyecto, ya que en esta etapa es en donde se establece el contexto organizacional y se analiza eventos futuros para gestionarlos. En la etapa de Ejecución del proyecto es en donde se manifiestan mayormente los impactos, los cuales pueden ser representados por pérdidas o salvaguardas económicas, como muestra la Figura 1.

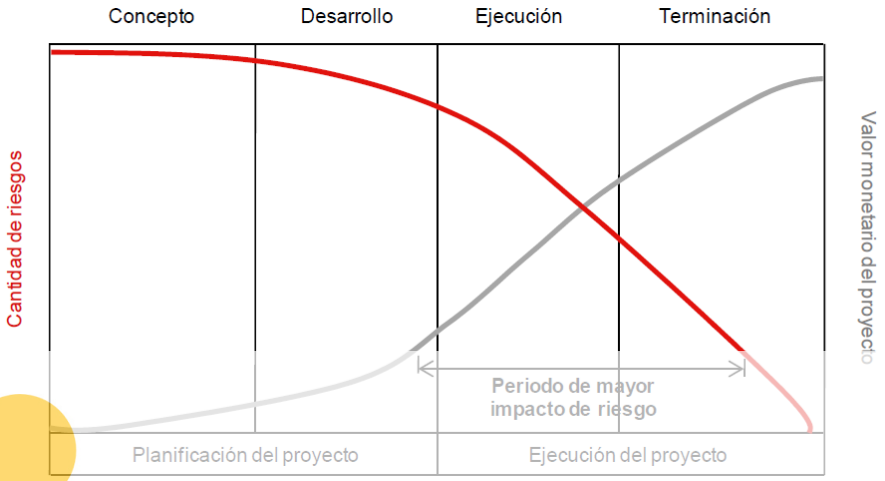

Figura 1. Relación Riesgo – Coste (PMI-PMBOK 4th Edición)

Tomando como referencia la Figura anterior, el riesgo es un elemento inherente en las etapas de planeación y ejecución de los proyectos, y al gestionarlos de forma proactiva se conseguirán mejores beneficios tanto para la organización como para el proyecto.

Por lo tanto, fundamentado en todo lo anterior, la gestión del riesgo implica planificación y análisis; identificación y mitigación; control y disminución del impacto de eventos que afecten la ejecución del proyecto.

Especialistas en el análisis y gestión del riesgo exponen los siguientes **factores a tomar en cuenta**:

- Boehm (1991): problemas con el personal, planificación temporal y presupuestos poco realistas.
- Ropponen y Lyytinen (1993): mala planificación del tiempo y requerimientos funcionales incorrectos.
- Jones (2005): métricas inexactas, medición inadecuada (métricas que perturban y ralentizan el proceso) y excesiva presión en la planificación.

Por tal motivo, contar con una metodología que gestione el Riesgo y que sirva de referencia a los profesionales y ejecutores de proyectos de TI es fundamental. Los modelos que conciernen a esta investigación son los que se muestran en la Tabla 1.

Tabla 1. Metodologías que Gestionan el Riesgo

METODOLOGÍA O MEJOR PRACTICA	DESCRIPCIÓN	ORGANIZACIÓN	PAIS
CMMI	Capability Maturity Model Integration	SEI (Software Engineering Institute)	Estados Unidos de América
SPICE	Software Process Improvement and Capability dEtermination	ISO (International Organization for Standardization)	Internacional (Suiza)
PMBOK	Project Management BOdy of Knowledge	PMI (Project Management Institute)	Estados Unidos de América
PRINCE2	Projects IN Controlled Environments	OGC (Office of Government Commerce)	Reino Unido
COBIT	Control OBjectives for Information and related Technology	ISACA (Information Systems Audit and Control Association) & ITGI (IT Governance Institute)	Estados Unidos de América
RISK IT	Risk IT Model	ISACA (Information Systems Audit and Control Association)	Estados Unidos de América
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation	Carnegie Mellon SEI (Software Engineering Institute) y CERT (Computer Emergency Response Team)	Estados Unidos de América
NIST 800-30	Risk Management Guide for Information Technology Systems	NIST (National Institute of Standards and Technology)	Estados Unidos de América
MAGERIT	Metodología de Análisis y GEstión de Riesgos de IT	MAP (Ministerio de Administraciones Públicas)	España

Para identificar las fortalezas y bondades de cada metodología se utilizará lo que hemos denominado **Elementos de Tecnología de Información o Elementos de TI**, que son áreas de especialidad en la ejecución de proyectos, siendo estos:

- Hardware [HW]
- Software [SW]
- Bases de Datos [BD]
- Redes y Telecomunicaciones [COM]
- Recurso Humano [RH]
- Legal [L]
- Financiero [F]
- Servicios [S]

La especificación de cada Elemento de TI se muestra en la Tabla 2.

Tabla 2. Elementos de Tecnologías de Información TI

ID	ELEMENTO DE TI	DESCRIPCION[4]
HW	Hardware	Equipos informáticos. Bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos. También se incluyen dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo. Pueden ser o no portátiles. Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
SW	Software	Con varias denominaciones (programas, aplicativos, desarrollos, etc.) se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. NOTA: El denominado "código fuente" o programas que serán datos de interés comercial a valorar y proteger como tales, serán considerado como datos.
BD	Bases de Datos	Elementos de datos, información que, de forma singular o agrupada representan el conocimiento que se tiene de algo. Almacenados en equipos o soportes de información. Pueden ser transferidos de un lugar a otro por los medios de transmisión de datos. Informes, líneas de texto denominados código fuente (Source code, code base) escrito en un lenguaje de programación específico.
COM	Redes y Telecomunicaciones	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.
RH	Recurso Humano	Personas relacionadas con los sistemas de información. Equipo de TI. Usuarios Internos y externos. Operadores, Administradores.
L	Legal	Contratos, Licenciamiento, Derechos de Autor. Ley de Trabajo (Contratación de Personal), Ley de Servicio de Rentas Internas (Impuestos). Seguridad de la información. Normativa de la Información.
F	Financiero	Procesos involucrados en estimar, presupuestar y controlar los costos de modo que se complete el proyecto dentro del presupuesto aprobado. También involucra procesos de estimación y control en cuanto a entrega y recepción de productos (bienes y servicios).
S	Servicios	Función que satisface una necesidad de los usuarios. Servicios de información, servicios de comunicaciones, servicios de seguridad, servicios de capacitación. Servicios requeridos para el eficaz desempeño de la misión del proyecto/ organización.

Para identificar el nivel de aceptación o correspondencia con los elementos de TI, se plantea una escala cuantitativa y cualitativa dividida en cuatro rangos diferenciando el nivel de satisfacción.

[44] MAGERIT

Los datos **cualitativos los denominamos Niveles de Puntuación (NP)** y los **datos cuantitativos decimos que se encuentran dentro de una Escala de Medición (EM).**

Al momento de seleccionar las actividades con mayor correspondencia, denominado **Rango de Selección**, se ha determinado dos alternativas de cumplimiento: **Satisfactorio (S)** e **Insatisfactorio (I).**

A continuación en la Tabla 3, se detalla la escala de valoración más los íconos de representación condicional:

Tabla 3. Escala de Valoración

ID	NIVEL DE PUNTUACION (NP)	ESCALA DE MEDICION (EM)	DESCRIPCION DE ALCANCE	RANGO DE SELECCIÓN	ÍCONOS DEL RANGO DE SELECCIÓN
N	NO CUMPLE	EM>=0 y EM <0.5	Indica que existe poca o nula correspondencia con el elemento de TI evaluado.	INSATISFACTORIO (I)	
P	PARCIAL	EM>=0.5 y EM <0.75	Muestra que existe aproximación pero algunas de las características con el elemento de TI no se dan.		
A	ADECUADO	EM>=0.75 y EM <1	El proceso alcanza correspondencia con el elemento de TI evaluado pero difiere o requiere algún aspecto.	SATISFACTORIO (S)	
C	CUMPLE	EM=1	Existe evidencia de que el proceso evaluado alcanza completamente o supera el nivel de correspondencia.		

La herramienta para tabular, calcular e integrar las funciones lógicas de los datos recolectados serán hojas electrónicas (Microsoft Excel V.2010). Esta técnica nos permitirá la representación condicional (íconos de los niveles alcanzados) y también incorporar gráficos de la información para realizar un análisis integral de los resultados obtenidos.

Como se puede apreciar en la Tabla 3, el nivel de puntuación **"No Cumple"**, abarca dos íconos de representación el cual considera que pueden existir valores igual a cero representados con el ícono vacío "○". De la misma manera existen dos íconos que representan el rango de selección **"Insatisfactorio"** puesto que este tiene dos puntuaciones que puede alcanzar, siendo estos "no cumple" o "parcial."

La sumarización de los datos obtenidos es el resultado de la aplicación de la siguiente ecuación:

$$EscalaDeMedición_{Metodología} = \frac{1}{np}\sum_{i=1}^{n} Xi \qquad (2)$$

Dónde n: es el Número Total de actividades que Gestionan el Riesgo

Xi: representa cada uno de los valores asignados

p: Elementos de TI ([HW], [SW], [BD], [COM], [RH], [L], [F], [S]), constante=8

El **proceso** a seguir (diseñado por el autor de este documento) para realizar la evaluación se basa en 3 **Fases**, de la siguiente manera:

1. Disgregación: Descomponer los modelos, metodologías y técnicas para determinar la característica o características encargadas de la Gestión del Riesgo.

2. Identificación: Identificar los procesos y actividades encargadas de la Gestión de Riesgos para someterlos a evaluación.

3. Evaluación: Realizar una comparación, sumarización y asignación cuantitativa y cualitativa de las actividades identificadas, bajo la escala de valoración de la Tabla 3 y ecuación (2) de este documento, con el objetivo de mostrar y estimar un nivel de correspondencia con los proyectos de TI.

3. Resultados y Discusión

En la Tabla 4 se presenta los resultados de la primera Fase, **Disgregación**. Por la diversidad de metodologías y con el fin de estandarizar los conceptos en este documento, la ***Categoría*** puede ser el tópico, tema o capítulo de la Metodología. Mientras que la ***Característica*** se refiere a la fase, área, dominio, grupo o macro-proceso.

Tabla 4. Categoría y Características de las metodologías que gestionan el Riesgo

METODOLOGÍA o MEJOR PRACTICA	CATEGORÍA	CARACTERISTICA QUE GESTIONA EL RIEGO
CMMI	Gestión de Proyecto	RSKM- Gestión de Riesgos
SPICE	Procesos de Proyecto	MAN.5 Gestión de Riesgos
PMBOK	Gestión de un proyecto	Gestión de los Riesgos del Proyecto
PRINCE2	Temática	Gestión del riesgo

METODOLOGÍA o MEJOR PRACTICA	CATEGORÍA	CARACTERISTICA QUE GESTIONA EL RIEGO
COBIT	Administración de Riesgos	• Planificar y Organizar (PO) • Entrega y Soporte (DS) • Mantener y Evaluar (ME)
RISK IT	Dominio	1. Gobierno del riesgo (RG) 2. Evaluación de riesgo (RE) 3. Respuesta de riesgo (RR)
OCTAVE	Fase	1. Visión de la organización 2. Visión tecnológica 3. Planificación de las medidas y reducción de los riesgos
NIST 800-30	Proceso	1. Análisis de Riegos 2. Gestión de Riesgos
MAGERIT	Proyecto AGR (Análisis y Gestión de Riesgos)	Análisis y Gestión de Riesgos

Por medio de la **Fase de Identificación** se logró separar los procesos encargados del Riesgo y especificar las actividades y estrategias para Gestionar el Riesgo de cada una de las metodologías consideradas en este documento. Una vez efectuada la **Fase de evaluación** de cada metodología, se obtuvo un conjunto de resultados que nos permiten analizar el nivel de correspondencia con los Elementos de TI y de las actividades que gestionan el riesgo por medio de una asignación cuantitativa y cualitativa a base de la escala de valoración de la Tabla 3. Por lo extenso de la información se presenta un ejemplo de resultados en la Tabla 5:

Tabla 5. Evaluación de Actividades que Gestionan el Riesgo - SPICE

ID	ACTIVIDADES QUE GESTIONAN EL RIESGO	ELEMENTOS DE TI								ACTIVIDAD				
		HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS	ESCALA DE MEDICION (EM)	NIVEL DE PUNTUACION (NP)		RANGO DE SELECCIÓN	
SP5.1	Establecer el alcance de la gestión de riesgos	0.5	1	0.75	0.5	0.5	0.5	1	0.75	0.69	P	◑	I	🟡
SP5.2	Definir estrategias de gestión de riesgos	0.5	1	0.75	0.5	0.75	0	0.75	0.75	0.63	P	◑	I	🟡
SP5.3	Identificar riesgos	1	1	1	0.75	0.5	0.5	0.75	1	0.81	A	◕	S	🟢
SP5.4	Analizar riesgos	0.5	0.75	0.75	0.5	0.5	0	0.75	0.75	0.56	P	◑	I	🟡
SP5.5	Definir y realizar acciones de tratamiento de riesgos	0.5	0.75	0.75	0.5	0.5	0.5	0.75	0.75	0.63	P	◑	I	🟡
SP5.6	Monitorizar los riesgos	0.5	0.75	1	0.5	0.5	0.5	0.5	1	0.66	P	◑	I	🟡
SP5.7	Tomar acciones preventivas o correctivas	0.5	0.75	1	0.5	0.5	0.5	0.75	0.75	0.66	P	◑	I	🟡
	SUMA TOTAL DE VALORES ASIGNADOS	4	6	6	3.75	3.75	2.5	5.25	5.75	4.63	N/A	N/A	N/A	N/A
	NUMERO TOTAL DE ACTIVIDADES	7	7	7	7	7	7	7	7	7	N/A	N/A	N/A	N/A
	ESCALA DE MEDICION (EM)	0.57	0.86	0.86	0.54	0.54	0.36	0.75	0.82	0.66	P	◑	I	🟡
	NIVEL DE PUNTUACION (NP)	P ◑	A ◕	A ◕	P ◑	P ◑	N ◔	A ◕	A ◕					
	RANGO DE SELECCIÓN	I 🟡	S 🟢	S 🟢	I 🟡	I 🟡	I 🔴	S 🟢	S 🟢					

Los resultados macro del **Nivel de Puntuación (NP)** alcanzado de todas las metodologías respecto a los elementos de TI, son los que se presentan en la Tabla 6:

Tabla 6. Nivel de Puntuación (NP) - Comparativa de Metodologías que Gestionan el Riesgo

MEJOR PRACTICA	ELEMENTO DE TI							
	HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS
CMMI	◑	◕	◕	◑	◑	○	◔	◑
SPICE	◑	◕	◕	◑	◑	◔	◕	◕
PMBOK	◑	◑	◑	◑	◕	○	◕	◑
PRINCE2	◑	◑	◑	◑	◑	◔	◔	◕
COBIT	◕	◕	◕	◕	◕	◕	◑	◕
RISK IT	●	◕	◕	◕	◕	◕	●	◕
OCTAVE	●	●	◕	●	◕	◕	◔	◑
NIST 800-30	●	◕	◕	●	◕	◕	●	◕
MAGERIT	◕	◕	◕	◕	◕	◕	◕	◕

LEYENDA: ○ No Cumple ◔ Parcial ◑ Adecuado ● Completo

A continuación, en la Tabla 7, se presenta los resultados comparativos del **Rango de Selección** alcanzado por cada metodología a base de la escala de valoración, es decir, su nivel de correspondencia frente a los Elementos de TI.

Tabla 7. Rango de Selección - Comparativa de Metodologías que Gestionan el Riesgo

MEJOR PRACTICA	ELEMENTO DE TI							
	HARDWARE	SOFTWARE	BASES DE DATOS	REDES Y TELECOMUNICACIONES	RECURSO HUMANO	LEGAL	FINANCIERO	SERVICIOS
CMMI	🟡	🟢	🟢	🟡	🟡	🔴	🔴	🟡
SPICE	🟡	🟢	🟢	🟡	🟡	🔴	🟢	🟢
PMBOK	🟡	🟡	🟡	🟡	🟢	🔴	🟢	🟡
PRINCE2	🟡	🟡	🟡	🟡	🟡	🔴	🔴	🟢
COBIT	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢
RISK IT	🟢	🟢	🟢	🟢	🟢	🟡	🟡	🟢
OCTAVE	🟢	🟢	🟢	🟢	🟢	🔴	🔴	🟡
NIST 800-30	🟢	🟢	🟢	🟢	🟢	🟡	🟡	🟢
MAGERIT	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢

LEYENDA: 🔴 Insatisfactorio 🟡 🟢 Satisfactorio

Los resultados cuantitativos de todo el proceso de evaluación se muestran en la siguiente Figura 2:

Enfoque UTE, V.4-N.2, Dic.2013: pp. 77 - 94
Recibido (Received): 2013/10/02
Aceptado (Accepted): 2013/12/13

http://ingenieria.ute.edu.ec/enfoqueute/
ISSN: 1390-6542

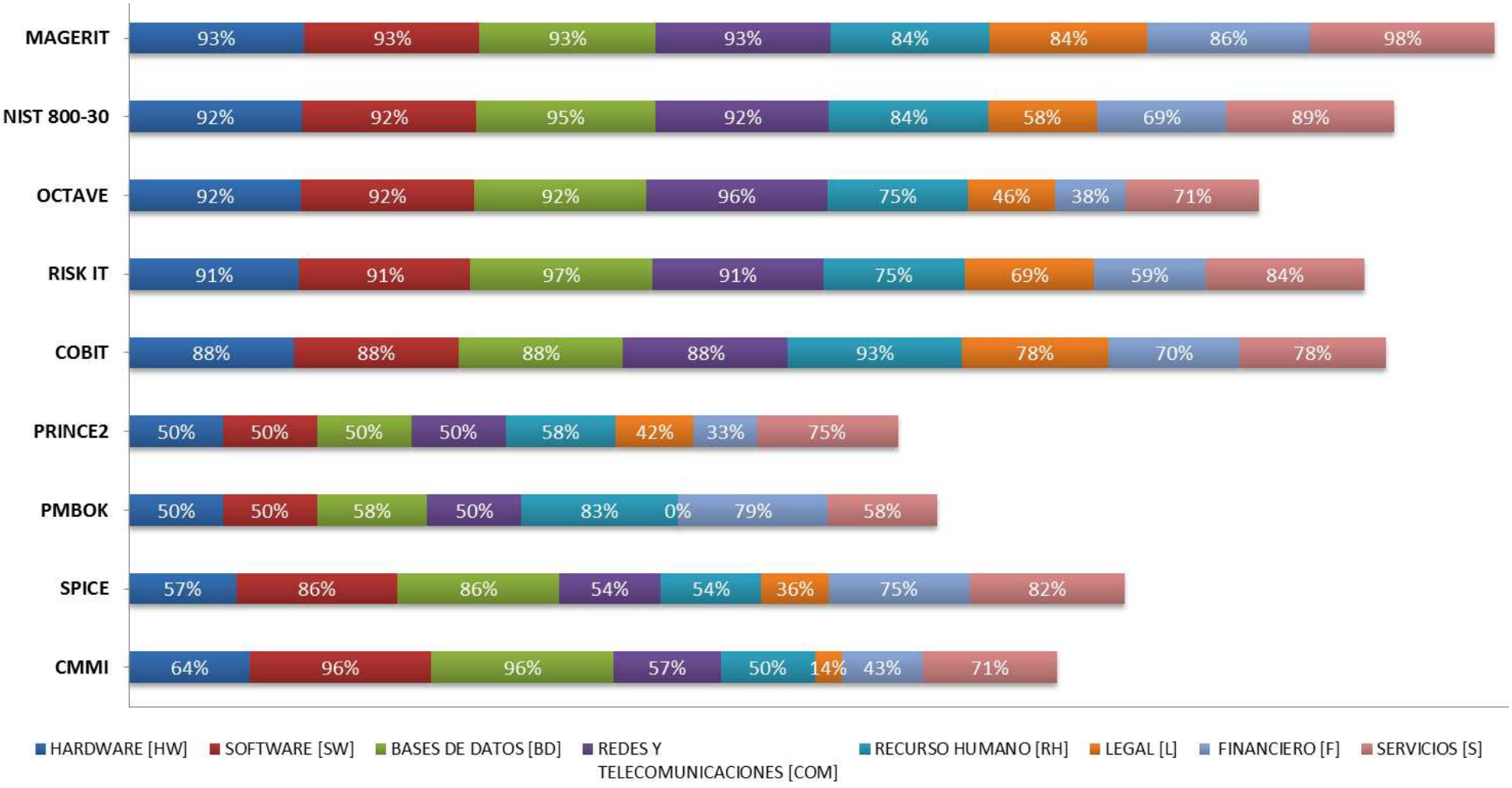

Figura 2. Comparativa de Mejores Prácticas que Gestionan el Riesgo – Escala de Medición (EM)

Enfoque UTE, V.4-N.2, Dic.2013: pp. 77 - 94
Recibido (Received): 2013/10/02
Aceptado (Accepted): 2013/12/13

http://ingenieria.ute.edu.ec/enfoqueute/
ISSN: 1390-6542

Tomando como base y referencia la **Tabla 6, Tabla 7 y Figura 2**, podemos destacar lo siguiente:

COBIT, RISK IT, OCTAVE, NIST 800-30 y MAGERIT alcanzan niveles de correspondencia satisfactorios al momento de Gestionar el Riesgo con respecto al: Hardware, Software, Bases de Datos, Redes y Telecomunicaciones. De igual manera CMMI y SPICE alcanzan el nivel satisfactorio cuando se trata de la Gestión del ciclo de vida del Software y Bases de Datos.

Aquellas metodologías que podemos destacar al momento de Administrar el Recurso Humano son PMBOK, COBIT, NIST 800-30 y MAGERIT. Estas metodologías al Gestionar el Riesgo matizan su acción definiendo un equipo de trabajo con perfiles y competencias para los proyectos, con su respectiva asignación de funciones y responsabilidades apoyadas por una matriz RACI[5] dando respuesta inmediata a los impactos sobre los objetivos del proyecto.

Respecto al tema Legal, COBIT y MAGERIT encabezan la lista cubriendo temas de Seguridad y Normativa de la Información. Sin embargo, una de las bondades que presenta MAGERIT es que la alineación de las leyes y normativas se basan según requerimientos técnicos-gubernamentales cubriendo temas que no tratan otras metodologías como: Contratos, Licenciamiento, Derechos de Autor, Contratación de Personal, Impuestos, Protección de datos de carácter personal, entre otros los cuales pueden servir como referencia según el área de aplicabilidad y ejercicio.

El trato con las finanzas, es un tema que las metodologías evaluadas en este artículo adolecen con la excepción de PMBOK y MAGERIT que sobrepasan el umbral definido en este documento. Un caso particular es COBIT y RISK IT los cuales son apoyados directamente por Val IT.

En cuanto a la correspondencia de los Servicios, cada modelo y metodología se orienta según su doctrina y ámbito de aplicación, por ejemplo CMMI y SPICE al desarrollo de aplicaciones y soluciones automatizadas, PMBOK y PRINCE2 a la gestión del proyecto; COBIT y RISK IT en la alineación de los objetivos de la organización con la Tecnología de la Información; OCTAVE, NIST 800-30 y MAGERIT en el Análisis y Gestión del Riesgo cuando se hace uso de la TI.

Según la Escala de Valoración de la Tabla 3, los valores considerados como satisfactorios son aquellos que alcanzan un valor igual o superior al 75%. A continuación, en la Figura 3 se presenta una consolidación integral de resultados utilizando la ecuación (1) de este documento:

[5] RACI, del inglés: Responsible, Accountable, Consulted, Informed (Responsable, Aprobador, Consultado, Informado)

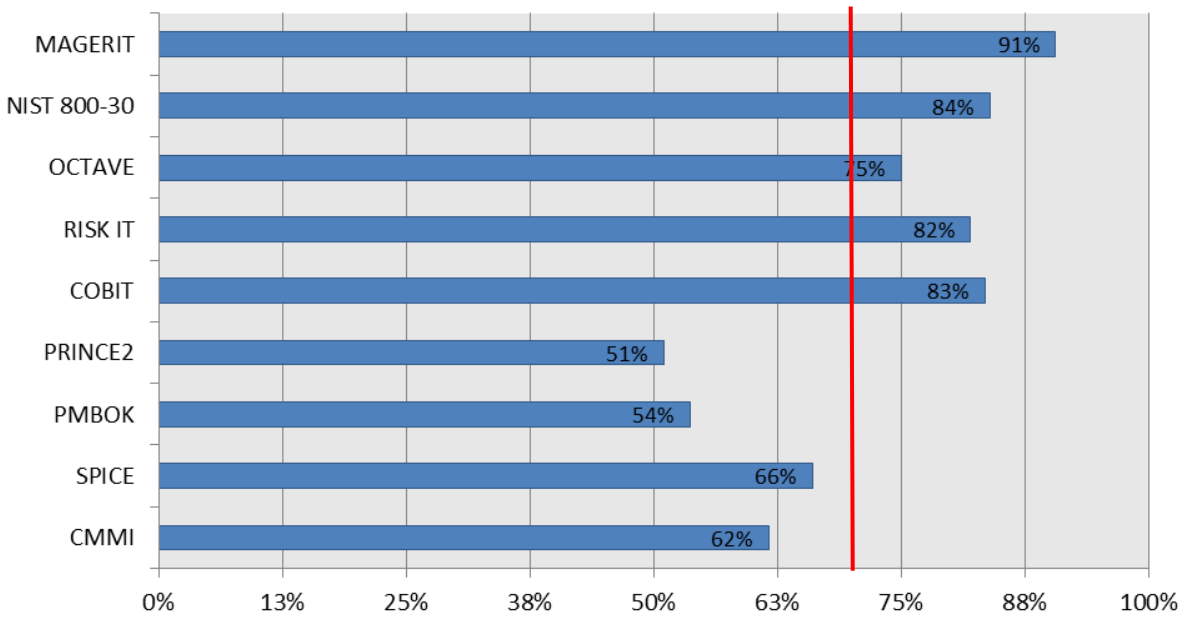

Figura 3. Metodologías que Gestionan el Riesgo - Consolidación de Resultados

Como se puede observar en la Figura 3, los valores alcanzados por MAGERIT (91%), NIST 800-30 (84%), COBIT (83%), RISK IT (82%) y OCTAVE (75%), demuestran que son metodologías que presentan alternativas que pueden ser consideradas por los administradores de contrato para gestionar el Riesgo en Proyectos de TI.

Todas las actividades de las metodologías correspondientes a esta investigación y que fueron sometidas a evaluación, se presentan en la **Figura 4**. Como se puede observar existen actividades que no satisfacen una correspondencia con las necesidades que se requieren cuando se ejecutan Proyectos de Tecnología de Información; sin embargo se puede destacar que existen actividades que apoyan su gestión y que están orientadas por ejemplo al Recurso Humano, al tema Legal y a las Finanzas como se aprecia en la Tabla 7.

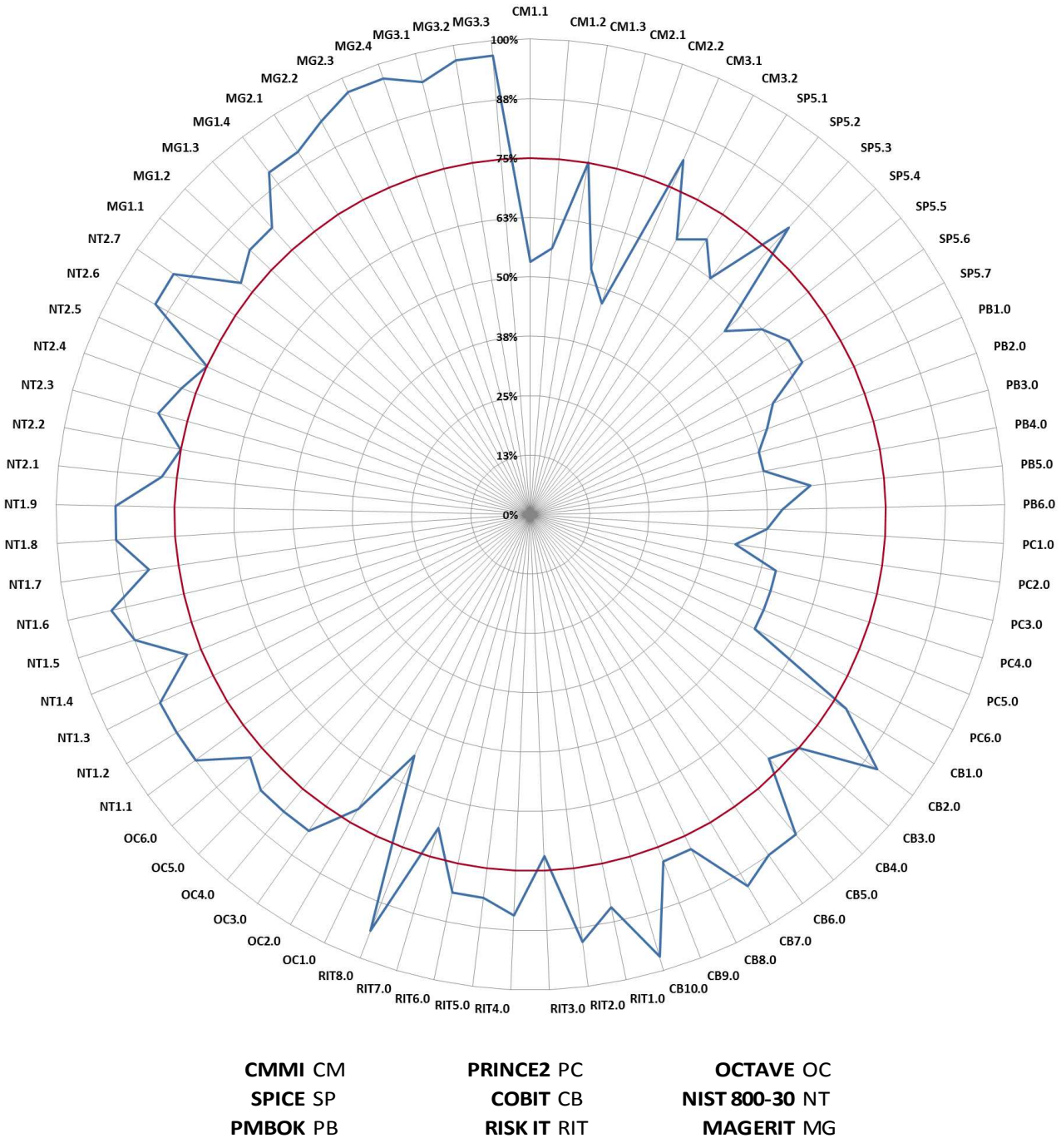

Figura 4. Metodologías - Actividades que Gestionan el Riesgo – Rango de Selección

4. Conclusiones y Recomendaciones

Las metodologías que se destacan al momento de gestionar el riesgo en Proyectos de TI y alcanzan niveles satisfactorios en Hardware, Software, Bases de Datos, Redes y Telecomunicaciones son MAGERIT, NIST 800-30, COBIT, RISK IT y OCTAVE. Esto se debe ya que en su estructura se establece criterios de seguridad, siendo los comunes entre estos la confidencialidad, integridad y disponibilidad que son la base para realizar el análisis y valorar la materialización de amenazas e impactos sobre los Elementos de TI.

En Software y Bases de Datos se destacan CMMI y SPICE por el soporte en la adquisición, desarrollo, operación y mantenimiento de productos de software. Respecto a la Administración del Recurso Humano PMBOK, COBIT, NIST 800-30 y MAGERIT alcanzan niveles satisfactorios, puesto que estas metodologías gestionan el riesgo definiendo un equipo de trabajo con perfiles, funciones y competencias para los proyectos con su respectiva asignación de roles y responsabilidades.

La administración de Normativa o legal y de la Seguridad de la información respecto a la Gestión del Riesgo la encabezan COBIT y MAGERIT. Esto es principalmente ya que COBIT cubre requerimientos de normas y seguridad mediante sus objetivos de control en base a las buenas prácticas a través de un marco de trabajo de dominios y procesos. MAGERIT por su parte, se alinea con las leyes y normativas técnicos-gubernamentales, cubriendo temas que no tratan otras metodologías como: contratos, licenciamiento, derechos de autor, contratación de personal, impuestos y protección de datos de carácter personal; siendo estos puntos referenciales para que los profesionales de TI puedan desarrollar el análisis de vulnerabilidades y amenazas en un proyecto al momento de Gestionar el Riesgo.

La Gestión del Riesgo al momento de administrar las finanzas, es un elemento que las buenas prácticas evaluadas en esta investigación adolecen por los resultados obtenidos, con la excepción de PMBOK y MAGERIT puesto que en su estructura tienen capítulos encargados de la planificar, estimar, presupuestar y administrar los costos de un proyecto. Un caso particular en este tema es COBIT y RISK IT ya que son apoyados directamente por Val IT.

La correspondencia de la Gestión del Riesgo de los Servicios de TI, cada metodología considerada en esta investigación se orienta según su doctrina y ámbito de aplicación, es decir, al desarrollo de aplicaciones y soluciones automatizadas, a la gestión del proyecto, en alinear las metas de negocio con las metas de Tecnología de la Información y al Análisis y Gestión del Riesgo cuando se hace uso de la TI.

Se recomienda a los profesionales que desarrollan y ejecutan proyectos de TI adquirir conocimientos de negociación, administración y finanzas. Aquellos profesionales que se encuentran ejecutando proyectos estatales es fundamental que conozcan la ley de contratación

pública, normas de control interno de la Contraloría y conocimientos básicos de permisos gubernamentales. Esto permitirá agilitar y desarrollar de manera eficiente los proyectos dentro de los parámetros y alternativas que las entidades públicas e instituciones del sector privado deben seguir.

Al momento de ejecutar Proyectos de TI, se recomienda conformar un equipo de trabajo especialista en cada área y que exista un responsable de Analizar y Gestionar el Riesgo. Regularmente, a más del Director del proyecto, se define un rol denominado Director de Riesgos de TI, quien es el responsable de supervisar todos los aspectos del Riesgo en uno o varios proyectos y es el encargado de presentar al Comité de proyecto o Directorio de la institución la información necesaria para una correcta toma de decisiones en cuanto al manejo del riesgo entorno a las salvedades y salvaguardas para minimizar pérdidas dentro de los parámetros técnico–legales.

Se recomienda continuar con esta línea de investigación para que la Gestión de Tecnologías de Información y Comunicaciones contenga técnicas de control y seguimiento elaboradas y propuestas por profesionales que se encuentran en el campo de acción y que con el apoyo de la alta dirección sean consideradas para incorporarlas en el interior de las entidades como una política de gestión.

Bibliografía

Galaway, L. (February 2004). *Quantitative Risk Analysis for Project Management: A critical review.* RAND Corporation working paper.

Boehm, B. (1991): *Risk management*. IEEE Software.

Ropponen y Lyytinen (1993): *Can Software Risk Management Improve System Development: An Exploratory Study*. European Journal of Information Systems

Jack A. Jones (2005): *An Introduction to Factor Analysis of Information Risk*. Risk Management Insight

Connell, S. (1997). *Desarrollo y Gestión de Proyectos Informáticos.* McGraw-Gill.

Software Engineering Institute. (2002). *CMMI* Capability Maturity Model Integrated

ISACA, Information Systems Audit and Control Association . (2007). *Control objectives for information and related technology COBIT® 4.1.*

ISACA, Information Systems Audit and Control Association. (2009). *The Risk IT Framework.*

ISO, International Organization for Standardization. (s.f.). *Software Process Improvement and Capability dEtermination, SPICE (ISO 15504).*

MAGERIT – Versión 2. (Junio 2006). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I Método, Libro II Catálogo de elementos, Libro III Guía de Técnicas.*

NIST, National Institute of Standards and Technology Special Publication 800-30. (July 2002). *Risk Management Guide for Information Technology Systems.*

OCTAVE, Operationally Critical Threat Asset and Vulnerability Evaluation. (June 9, 2003). *Method Implementation Guide Version 2.0.*

Office of Government Commerce. (2002). *Projects IN Controlled Environments, PRINCE2 Manual* (3rd Edition ed.). Londres.

Project Management Institute, 4th Edition. (s.f.). *A Guide to the Project Management Body of Knowledge PMBOK.*